UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
(ALEXANDRIA DIVISION)

GLOBAL POLICY PARTNERS, LLC, *et al.*,	
Plaintiffs,	
	Civil Action No. 1:09-cv-859 TSE/TRJ
vs.	
BRENT YESSIN, *et al.*,	
Defendants.	

PLAINTIFFS' OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

Plaintiffs Global Policy Partners, LLC ("GPP") and Katherine Friess Yessin ("Ms. Friess Yessin") (collectively, "Plaintiffs"), by and through their undersigned counsel of record, respectfully submit this Opposition to Defendant Brent Yessin's Motion to Dismiss ("Motion").

INTRODUCTION

In his Motion, Defendant relies upon knowingly false Annual Reports that are outside the pleadings in order to convince the Court that, as the ***sole*** Manager of GPP, he was "authorized" to commit Federal and State computer crimes. Defendant then forum-shops by referring the Court to a baseless declaratory relief action that he filed ***after*** this action was filed and served in order to invite the Court to stay these proceedings. Defendant makes these arguments by interjecting facts and documents that are outside the pleadings and by attempting to dispute facts alleged in Plaintiffs' Complaint.

Plaintiffs brought this action against Defendant for multiple violations of Federal and State law arising from Defendant's unlawful electronic interception and surveillance of

Plaintiffs' computer and electronic email accounts and misappropriation of Plaintiffs' confidential and proprietary business information, personal information, and privileged attorney-client communications. In violation of Federal and State criminal law, Defendants conducted this unlawful surveillance and obtained privileged attorney-client communications in order to, *inter alia*, harm GPP and Ms. Friess Yessin and obtain an unfair advantage in the pending divorce proceedings between Ms. Friess Yessin and Defendant. Defendant's actions violate provisions of the Federal Computer Fraud and Abuse Act (the "CFAA"), Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the "FWA"), Title II of the Electronic Communications Privacy Act (the "ECPA"), 18 U.SC. § 2701 *et seq*., and Virginia Code Ann. §§ 18.2-152.3; -152.4; -152.5, -152.12, and § 19.2-62 and -69 (the "VCAA").

In their Original Complaint, Plaintiffs repeatedly alleged that Defendant did not have the authority to conduct the unlawful interception and surveillance alleged in the Complaint, and these allegations must be accepted as true. In his Motion, Defendant attempts to dispute these allegations by interjecting the fact that he was the ***sole*** Manager and, as such, he had the authority to do whatever he wants. This contention is contrary to Plaintiffs' allegations and the governing law. Indeed, even if the Court were to, as Defendant invites, disregard Plaintiffs' allegations and consider Defendant's interjected facts and knowingly false documents, as a Manager he still did not have the authority to conduct the unlawful interception and surveillance alleged in Plaintiffs' Complaint.

In addition to his claim that he had such authority, Defendant makes a few technical challenges to Plaintiffs' claims. Specifically, that: (1) with respect to Plaintiffs' CFAA claims, Plaintiffs have failed to allege damage or loss (Motion at 9-14); (2) with respect to Plaintiffs' VCCA claims, Plaintiffs have failed to allege that Defendant "obtained, embezzled or converted"

Plaintiffs' property and "viewed her employment or other financial information" (*id.* at 14-15); and (3) with respect to Plaintiffs' FWA and VCCA claims, Plaintiffs have failed to allege that Defendant "intercepted any electronic communications during transmission" (*id*. at 17-20). Although Plaintiffs contend that they alleged sufficient facts in their Original Complaint to sustain all these claims, out of an abundance of caution, on September 17, 2009 Plaintiffs filed an Amended Complaint which clarifies their claims and addresses these alleged infirmities.[1] Thus, Defendant's arguments based upon these alleged technical deficiencies are now moot.

Finally, relying upon knowingly false documents, Defendant contends that Plaintiffs lack standing to bring this action and, based on a baseless declaratory relief action that he filed ***after*** this action was filed and served, Defendant asks the Court to stay this action. For the reasons set forth below, the Court should reject Defendant's forum-shopping and deny his Motion in its entirety.

ARGUMENT

I. Legal Standards

The Court may dismiss claims under Rule 12(b)(6) only if the Complaint does not "allege 'enough facts to state a claim to relief that is plausible on its face.'" *Ruttenberg v. Jones*, 283 Fed. App. 121, 128 (4th 2008) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). The Court must accept all facts alleged in the Complaint as true and "draw all reasonable factual inferences from those facts in the [Plaintiffs'] favor." *Edwards v. City of Goldsboro*, 178 F.3d 231, 244 (4th Cir. 1999).

The Motion before the Court is one filed pursuant to Rule 12(b)(6) and Defendant's

[1] For the convenience of the Court and counsel, the numbered paragraphs are the same in both the Original and Amended Complaints. In addition, although well pled, Plaintiffs have withdrawn their trespass to chattels claim.

extraneous documents and interjected facts should be ignored. Under Rule 12(d), a motion to dismiss may not be accompanied by "matters outside the pleadings," and the Court should exclude any such material. If the Court does not exclude those matters, then the motion "must be treated as one for summary judgment under Rule 56." Fed. R. Civ. P. 12(d). But, merely appending materials to a motion to dismiss does not properly convert it to one for summary judgment because such a rule would "conflict[] with Rule 12(b)(6)'s requirement that a court provide parties with notice of its intention to treat a motion to dismiss as one for summary judgment and a reasonable opportunity to present all material made pertinent to such a motion by Rule 56." *Finley Lines Joint Protective Board Unit 200 v. Norfolk S. Corp.*, 109 F.3d 993, 996 (4th Cir. 1997) (citation and internal quotation marks omitted); *see also* Fed. R. Civ. P. 12(d). Thus, if the Court elects to treat Defendant's Motion as a Rule 56 motion, then the Court should first give the parties notice that it intends to convert the Motion, so the parties can then address the Motion in the posture the Court has requested. *See e.g.*, *Johnson v. RAC Corp.*, 491 F.2d 510, 513 (4th Cir. 1974).

If the Court elects to convert Defendant's Motion into one for summary judgment, at that point, Plaintiffs would brief their response in accordance with this Court's typical procedures for addressing Rule 56 motions, including a Rule 56(f) motion and affidavit for discovery. *See* Fed. R. Civ. P. 56(f). This would be expected since no discovery has been taken in this case.

II. Defendant Was Not Authorized To Commit The Computer Crimes Alleged In Plaintiffs' Complaint

A. In Their Complaint, Plaintiffs Have Alleged That Defendant Acted Without Authorization

Relying upon factual assertions and documents outside the pleadings, the thrust of Defendant's Motion is that he had authorization to commit the computer crimes alleged in

Plaintiffs' Complaint. The fatal infirmity with this argument is that Plaintiffs have repeatedly alleged that Defendant lacked this authority. Specifically, Plaintiffs have alleged that:

- GPP operates under strict standards of confidentiality and "strictly protects and maintains the confidential and proprietary nature of its trade secrets, software, documents, communications, and services with passwords and other safeguards." Complaint, ¶ 10;

- "GPP limits access to its computer system by assigning usernames and passwords to all GPP authorized users." *Id*. at ¶ 14; *see also id.* at ¶¶ 31, 41;

- "Defendant was not an authorized user on the GPP computer and email system and he did not have a GPP email account, email address, or password." *Id*. at ¶ 14; *see also id.* at ¶¶ 31, 41;

- "Without authorization or consent, Defendant broke into Ms. Friess Yessin's GPP email account and unlawfully surveilled her business and personal documents and communications, including very sensitive, privileged communications with her counsel regarding her strategy in her impending divorce proceedings with Defendant." *Id*. at ¶ 16; *see also id.* at ¶¶ 33, 35, 43-45, 51, 59, 67, 75, 83, 92, 99, 106, 113, 121-22, 131-33;

- "None of Defendant's . . . unauthorized actions as described in this Complaint are reasonably related, in any form whatsoever, to the rendering of services, or performance of any duties, on behalf of GPP. To the contrary, at all times relevant to this Complaint, Defendant was acting for his own individual personal gain." *Id*. at ¶ 27;

- "Defendant . . . had no authority to authorize or engage in the criminal unlawful surveillance that is the subject of this Complaint." *Id*. at ¶ 12; and

- "Defendant has conducted this unlawful surveillance to, *inter alia*, harm Ms. Friess Yessin and GPP and obtain a decisively unfair advantage in the pending divorce proceedings between him and Ms. Friess Yessin." *Id*. at ¶ 26; *see also id.* at ¶¶ 23-25, 36-37, 46-47, 54-55, 62-63, 70-71, 79-80, 88-89, 94-95, 101-02, 108-09, 115-16, 123, 126-27, 135-37.

Plaintiffs have repeatedly alleged that Defendant conducted the unlawful interception and surveillance without Plaintiffs' authorization for the improper purposes of harming GPP and obtaining Ms. Friess Yessin' privileged communications with her counsel in order to obtain an unfair advantage in another litigation. At this juncture, these facts must be accepted as true. *See*

Section I, *supra*. Indeed, given that Defendant was not an authorized user on the GPP computer and email system and he did not even have a GPP email account, email address, or password, he cannot now go beyond the pleadings and contend that he had such access or authorization.

B. Defendant Cannot Dispute Plaintiffs' Allegations By Interjecting And Relying Upon Knowingly False Facts And Documents

Instead of accepting Plaintiffs' allegations as true, Defendant interjects that as the ***sole*** Manager of GPP he had authority to commit the crimes alleged in Plaintiffs' Complaint. To make this argument, Defendant relies on knowingly false Annual Reports that he alone executed and filed with the Florida Secretary of State. The problem for Defendant is that the very law he cites in his Motion makes clear that he had no such authority to make these filings.

As alleged in the Complaint, GPP is a Limited Liability Company governed by Florida Law. Complaint, ¶ 5. A Florida Limited Liability is governed by its Members and/or Managers. Fla. Stat. Ann. § 608.422. As alleged in the Complaint, Ms. Friess Yessin and Mr. Weiss are the majority Members and 2 of the 3 Managers. Complaint, ¶ 12. As alleged in the Complaint and as Defendant's Motion correctly states, GPP's Articles of Organization provide that there are three Managers – Ms. Friess Yessin, Jeffrey Weiss, and Defendant. Complaint, ¶ 12; Motion at 7-8; Exhibit 5 to Motion. As Defendant's Motion also correctly states, "[a]ny matter relating to the business of the limited liability company may be exclusively decided by the manager or, ***if there are more than one managers, by a majority of the managers***," Motion at 8 (citing Fla. Stat. Ann. § 608.422(4)(b) (emphasis added)). Since the Articles of Organization that Defendant relies upon provide that GPP had 3 Managers, then business decisions are made by a majority of them – here, 2 out of the 3 Managers. Thus, Defendant's contention that he had "decision making authority" and rights "equal" to the combined vote of Ms. Friess Yessin and Mr. Weiss is contrary to Plaintiffs' allegations and the Florida law he cites in his Motion. Motion at 7-10. As

1 of 3 Managers, Defendant simply could not be authorized to engage in the unlawful interception and surveillance alleged in Plaintiffs' Complaint.[2]

Realizing that this is the case, in his Motion, Defendant also contends that he is the ***sole*** Manager and, thus, had the authority to commit computer crimes. Motion at 2-3, 8, 21, 24. To support this argument, Defendant attaches and relies upon two Annual Reports that he alone created, executed under oath, and filed with the Florida Secretary of State -- the April 30, 2008, Annual Report which purports to ***delete*** Ms. Friess Yessin and Mr. Weiss as Managers (Exhibit 4 to Motion) and the April 2, 2009 Annual Report that falsely claims under oath that he is the sole Manager (Exhibit 1 to Motion). Motion at 2-3, 8, 21 & Exhibits 1 & 4. Defendant alone executed and filed these Annual Reports subject to penalty of perjury without the knowledge or authorization of Ms. Friess Yessin and Mr. Weiss.

But Defendant has missed a step. Conspicuously absent from Defendant's Motion is how he, as a minority Member and only 1 of 3 Managers, could "delete" the other two Managers to enable him to have "authorization" to commit computer crimes. Florida law expressly provides that a Manager "[m]ust be . . . removed, or replaced by a vote, approval or consent of a majority-in-interest of the members . . ." Fla. Stat. Ann. § 608.422(4)(c)(1). Florida law also provides that "[n]otwithstanding any provision to the contrary in the articles of organization or operating

---

[2] The same would be true if GPP were a Member-managed LLC. Under Florida Law, "[m]anagement shall be vested in its members or elected managing members in proportion to the then-current percentage or other interest of members in the profits of the limited liability company owned by all of the members or elected managing members." Fla. Stat. Ann. § 608.422(2)(a). Florida law also provides that "[e]xcept as otherwise provided in subsection (3) [which addresses where the Articles of Organization provide for management of the LLC by its Managers] or in this Chapter, the decision of a majority-in-interest of the members or elected managing members shall be controlling." *Id.* at § 608.422(2)(b). As alleged in the Complaint, Ms. Friess Yessin and Mr. Weiss are the majority Members of GPP. Complaint, ¶ 12. Thus, if GPP were a Member-managed LLC, then they – and not Defendant – control the business of GPP and would be in control of decisions made on its behalf.

agreement, in no event shall the articles of organization be amended by a vote of less than a majority-in-interest of the members." Fla. Stat. Ann. § 608.4231(4). In their Complaint, Plaintiffs have specifically alleged that they were the majority Members. Complaint, ¶ 12. As a minority Member and only 1 of 3 Managers, Defendant could not possibly have unilaterally amended the Articles of Organization by filing false Annual Reports that remove or otherwise "delete" the other two Managers. Fla. Stat. Ann. § 608.422(4)(c)(1); Fla. Stat. Ann. § 608.4231(4). Defendant filed these Annual Reports under oath and affirmed that they were "true and accurate", even though he knew that could not be the case. Now, he submits them to this Court in order to avoid liability for his computer crimes.

Put simply, as a minority Member and only 1 of 3 Managers, Defendant did not have the authority to conduct the surveillance alleged in the Complaint and he cannot interject facts and knowingly false Annual Reports in order to manufacture such authority. At best, Defendant has presented a factual dispute that may be resolved only after discovery has been completed.

C. Even As A Manager, Defendant Was Not Authorized To Commit The Computer Crimes Alleged In Plaintiffs' Complaint

Even if the Court disregards Plaintiffs' allegations, as a Manager Defendant still was not authorized to surveill Plaintiffs for the improper, ***non-business*** purposes of harming GPP and obtaining Ms. Friess Yessin's attorney-client communications so he could use them against her in another litigation. In his Motion, Defendant argues that, as a Manager, he was authorized to access GPP's computer system for ***any*** purpose and that this access was not subject to ***any*** limitations. Motion at 9-11. These assertions are contrary to Plaintiffs' allegations and the governing law. In their Complaint, Plaintiffs have specifically alleged that GPP operates under strict standards of confidentiality and "GPP limits access to its computer system by assigning usernames and passwords to all GPP authorized users." Complaint, ¶ 14; *see also id.* at ¶¶ 31,

41. Plaintiffs also have alleged that "Defendant was not an authorized user on the GPP computer and email system and he did not have a GPP email account, email address, or password." *Id*. Given that Defendant was not even permitted to use the GPP email system and did not have an email account, email address or password, he cannot go beyond the pleadings and contend that he did and was authorized to access GPP's computer and email systems.

In his Motion, Defendant has failed to cite any authority which stands for the proposition that a Manager of an LLC automatically has unfettered access to all areas of a company's computer system or network merely by virtue of being a Manager. Defendant also cites no authority for the proposition that a Manager of a LLC has authority to access the password-protected email account of another Manager without her knowledge or authorization. His only claim is that his authority to access the GPP computer system, and Ms. Friess Yessin's email account, derives from Fla. Stat. Ann. § 608.4235 (2009). Motion at 10. This statute merely provides that any Manager may "sign and deliver any instrument transferring or affecting the company's interest in real property." Notably, the statute does not address access to company computer systems. As stated above, "[a]ny matter relating to the ***business***" of GPP is decided by a majority of its Managers. Fla. Stat. Ann. § 608.422(4)(b) (emphasis added). Managers are entrusted with conducting the ***business*** of the LLC. *Id*. Conducting unlawful interception and surveillance to harm GPP and to spy on another Manager in order to obtain the upper hand in a pending litigation are obviously not legitimate business purposes. Indeed, although he interjects reams of other facts, nowhere in Defendant's Motion is there any suggestion that Defendant conducted the surveillance for a legitimate business purpose. Thus, even if Defendant had certain rights as a minority Manager, nothing in the Florida statutory scheme gave him access to GPP's computer network and, in particular, to Ms. Friess Yessin's password-protected GPP

email account.

III. Plaintiffs Have Stated Claims Under The CFAA – Counts I And II

In his Motion, Defendant asserts that Plaintiff has not stated claims under the CFAA – Counts I and II – because: (1) Defendant was not an "outsider" and that, as a Manager, he was authorized or did not exceed authorized access to commit the computer crimes alleged in Plaintiffs' Complaint; and (2) Plaintiffs have failed to allege facts showing "damage or loss." Motion at 9-14.

A. Defendant Did Not Have Authorization

As discussed at length in Section II above, Plaintiff has specifically alleged that Defendant did not have authority to conduct the unlawful surveillance alleged in the Complaint, and those allegations must be accepted as true. *See* Sections I & II, *supra*.

The CFAA prohibits the intentional accessing of a computer "without authorization or exceeding authorized access" to obtain information from a "protected computer" if the conduct involved an interstate or foreign communication. § 1030(a)(2)(C). The phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." § 1030(e)(6). Congress did not define "unauthorized access" in the statute.

Courts vary as to how broadly or narrowly to construe the CFAA. Some courts have held that the CFAA is primarily concerned with "computer hackers" (*e.g.*, electronic trespassers), *State Analysis, Inc. v. American Financial Services Assocs.*, 621 F. Supp. 2d 309, 315 (E.D. Va. 2009) (citing *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000)), and only applies to situations "where an outsider, or someone without authorization, accesses a computer." *Id.* (*Citing In re AOL, Inc. Version 5.In re AOL, Inc.*

Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1370 (S.D. Fla. 2001)). These authorities have rejected attempts to apply the CFAA to circumstances where the defendants are not alleged to have "broken into" the system, but to have abused the privileges of a license. Other courts, however, have held that the CFAA does apply to authorized users who use programs in an unauthorized way, including employees who obtain and use proprietary information in violation of a duty of loyalty, *id*. at 316 (citing *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006), and licensees who breach an agreement restricting their use of the software, *Modis v. Bardelli*, 531 F. Supp. 2d 314, 319 (D. Conn. 2008).[3]

In *State Analysis*, Judge Brinkema denied a defendant's motion to dismiss the plaintiff's CFAA and ECPA claims where, according to the complaint, defendant Kimbell Sherman Ellis ("KSE"), a government relations and public affairs firm, accessed password-protected areas of plaintiff's website using usernames and passwords that did not belong to it – the plaintiff had alleged that only clients were authorized to use their subscription services and KSE was not so authorized. 621 F. Supp. 2d at 316, 317.[4]

---

[3] The Fourth Circuit has yet to opine as to whether it applies a narrow or broad interpretation of the CFAA. Although this Court has not expressly adopted either interpretation, it appears to take a more narrow interpretation of the statute. *See, e.g.*, *State Analysis*, 621 F. Supp. 2d at 316; *SecureInfo Corp. v. Telos Corp*., 387 F. Supp. 2d 593, 608, 609-10 (E.D. Va. 2005). Under either interpretation, Plaintiffs have stated a viable claim under the CFAA because the Complaint unequivocally alleges that Defendant was not authorized to access the GPP computer network nor Mrs. Friess Yessin's password-protected email account, and that he "broke" into that account. Complaint, ¶¶ 10, 14, 16, 31-35, 41-45; *see also id*. at ¶¶ 12, 14, 16, 27, 51, 59, 67, 75, 83, 92, 99, 106, 113, 121-22, 131-33.

[4] KSE had obtained usernames and passwords from the co-defendant in the case, American Financial Services Association ("AFSA"). AFSA was a business association and was a client of the plaintiff. Although the Court denied KSE's motion to dismiss, the court did, however, grant AFSA's motion to dismiss the plaintiff's CFAA and ECPA claims, finding that AFSA's access to plaintiff's website was authorized. The Court observed that the plaintiff did not allege that AFSA had ***accessed*** information it was not entitled to, but rather alleged that AFSA had ***used*** such information in an inappropriate way. As such, the Court concluded that the plaintiff had not stated a claim for a violation of the CFAA or ECPA against AFSA. 621 F. Supp. 2d at 317, 318.

Defendant's Motion likewise should be denied because, as in *State Analysis*, Plaintiffs operate under strict standards of confidentiality, Plaintiffs have alleged that GPP strictly limits access to its computer system by assigning usernames and passwords to all GPP authorized users, Defendant was not an authorized user on the GPP computer and email system and he did not have a GPP email account, email address, or password, and that, without authorization, he broke into password-protected areas of GPP's email system using a username and password that did not belong to him. Complaint, ¶¶ 10, 14, 16, 31-35, 41-45; *see also id*. at ¶¶ 27, 51, 59, 67, 75, 83, 92, 99, 106, 113, 121-22, 131-33.[5] Although Defendant argues that the statute is intended to target "hackers" or "outsiders, or someone without authorization" (Motion at 9), Plaintiffs have specifically alleged that, for purposes of his crimes, this is precisely what Defendant was. Complaint, ¶¶ 10, 14, 16, 31-35, 41-45.

As noted above, Congress did not define the phrase "unauthorized access" in the CFAA. A number of courts have analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user. Applying this "intended-use" analysis, in *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991), the Second Circuit held that transmission of an internet worm designed "to demonstrate the inadequacies of current security measures on

---

Here, Plaintiffs have asserted that Defendant unlawfully intercepted and ***accessed***, not merely used, information to which he was not entitled. Complaint, ¶¶ 10, 12, 14, 16, 31-35, 41-45.

[5] Given that Plaintiffs have specifically alleged that Plaintiffs operate under strict standards of confidentiality, GPP strictly limits access to its computer system by assigning usernames and passwords to all GPP authorized users, and that Defendant was not an authorized user on the GPP computer and email system and he did not have a GPP email account, email address, or password, Defendant's assertions that "Plaintiffs do not allege that GPP has any formal policies limiting a manager's access to company property or computer systems", that "the Company operates on a policy of unlimited access", and that he had "unlimited" access (Motion at 10) are without merit and contrary to Plaintiffs' allegations.

computer networks by exploiting . . . security defects" was sufficient to permit a jury to find unauthorized access within the meaning of Section 1030(a)(5)(A). *Morris*, 928 F.2d at 505.

The *Morris* court concluded that conduct such as "password guessing" or finding "holes in . . . programs," that use computer systems not "in any way related to their intended function" amounts to obtaining unauthorized access. *Id*. at 510; *see also United States v. Phillips*, 477 F.3d 215, 220 (5th Cir. 2007) (holding that the defendant's "brute-force attack program" was not an intended use of the University network within the understanding of any reasonable computer user and constituted a method of obtaining unauthorized access to computerized data that he was not permitted to view or use); *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004) (internet site administrator's misappropriation of login names and passwords to obtain access to competitor's website violated CFAA); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1074 (9th Cir.), *cert. denied*, 543 U.S. 813 (2004) (use of an authorized third-party's password by an outside hacker to gain access to a mail server fell within "the paradigm of what [Congress] sought to prohibit [under the Stored Communications Act]").

Applying the intended-use analysis to the facts alleged here, Defendant's actions were not consistent with the expected norms of the relationship between him, GPP, and the other Managers. Here, the Complaint expressly alleges that Defendant had no authority to access GPP's computer and email system, and in particular, he had not authority to access Ms. Friess Yessin's GPP email account. Complaint, ¶¶ 10, 14, 16, 31-35, 41-45; *see also id*. at ¶¶ 27, 51, 59, 67, 75, 83, 92, 99, 106, 113, 121-22, 131-33. Since Defendant had no GPP email account, email address, or password of his own and was not even permitted access to the system, he was not authorized to conduct the unlawful surveillance alleged in Plaintiffs' Complaint.

B. **Plaintiffs Have Sufficiently Alleged Damage And Loss**

18 U.S.C. § 1030(g) provides that one "who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."

1. Plaintiffs Have Alleged "Loss"

In accordance with Section 1030(g), Plaintiffs have sufficiently alleged "loss". A plaintiff's "loss" must aggregate at least $ 5,000 under this statute, and "loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Defendant argues that the final four words of this provision, "because of interruption of service," modifies the entire definition of "loss." Motion at 13. Therefore, under Defendant's construction of this statute, "any reasonable cost" incurred by a victim, to be recoverable, must be "incurred because of interruption of service." To support this narrow reading of the statute, Defendant relies on a case from the Southern District of Florida, *The Continental Group, Inc. v. KW Property Mgmt, LLC,* 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009), and in so doing, overlooks recent case law from the Fourth Circuit that is directly on-point and which does not comport with Defendant's desired interpretation.

In *A.V. v. iParadigms, LLC,* 562 F.3d 630, 646 (4th Cir. Va. 2009), the Court did not limit "loss" under §1030(e)(11) to costs only associated with interruption of service, and stated:

> This broadly worded provision plainly contemplates consequential damages of the type sought by iParadigms -- costs incurred as part of the response to a CFAA violation, including the investigation of an offense. *See, e.g., Modis, Inc. v. Bardelli,* 531 F. Supp. 2d 314, 320 (D. Conn. 2008) (noting that "the costs of

> responding to the offense are recoverable" including "costs to investigate and take remedial steps" (internal quotation marks omitted)); *SuccessFactors, Inc. v. Softscape, Inc*., 544 F. Supp. 2d 975, 980-81 (N.D. Cal. 2008) (holding that the cost of investigating and identifying the CFAA offense, including "many hours of valuable time away from day-to-day responsibilities, causing losses well in excess of $ 5,000," qualified as "cost[s] of responding to an offense" under § 1030(e)(11)).

Nothing in this opinion indicates that any of iParadigm's losses arose out of interruption of service. To the contrary, the focus of the Court was on other consequential damages, including investigative and remedial expenses, and could even include loss of goodwill *Id*.

Similarly, in *CoStar Realty Info., Inc. v. Field*, 612 F. Supp. 2d 660, 674-75 (D. Md. 2009), a real estate database service, CoStar, sued two individuals who were using its website without authorization—by illicitly using a paying subscriber's username and password. CoStar argued that it suffered damages based on loss of revenue from the failure to recover license fees. *Id*. at 674. The Complaint alleged that "unauthorized access of a protected computer has caused damage to CoStar that has amounted in an aggregate loss of over $ 5,000 during a one-year period," as well as loss of revenue from its license fees due to Defendants' unauthorized use of CoStar's database. *Id*. at 675. Defendants moved to dismiss on the grounds that the plaintiff had not alleged loss as the result of "interruption of service," because CoStar still maintained use of its database during Defendant's unauthorized conduct. *Id*. at 675.

The Court denied the defendant's motion. In doing so, it noted a circuit split over the construction of the "interruption of service" provision. *Id*. It cited to *Frees, Inc. v. McMillian*, No. 05-1979, 2007 U.S. Dist. LEXIS 57211 at *15-16 (W.D. La. Aug. 6, 2007) where "the court noted that in order to claim under the CFAA one must establish the jurisdictional threshold for loss, by alleging facts that constitute loss," and that the term "loss" was a term of art that was not intended to control or limit what damages are recoverable in a civil action. *Id*. at 675 (*also citing*

Therapeutic Research Faculty v. NBTY, Inc., 488 F Supp. 2d 991, 996-97 (E.D. Cal. 2007) (holding loss alleged where loss entailed unauthorized name of user name and password, in violation of a software license agreement)). The *CoStar* Court joined *Frees* and *Therapeutic Research Faculty* in holding that the plaintiffs had properly alleged "loss" under Section 1030. *Id*.

Finally, in *State Analysis*, relied on by the Defendant in other arguments in his Motion - and the case in which Defendant's attorney was lead counsel for the defense - this Court properly focused on the "any reasonable cost" clause, as opposed to the "interruption of service" clause, when it summarized the definition of loss: "The CFAA allows a plaintiff to recover for 'loss,' defined as 'any reasonable cost to any victim . . .' as well as 'damage' . . . ." *State Analysis*, 621 F. Supp. 2d at 316 (ellipses in original).

In accordance with the above authority, "loss" under §1030(e)(11) includes the costs of responding to a violation, including costs of investigation, remediation, time away from the business (owner's opportunity cost), lost revenue, and loss of goodwill. In their Complaint, Plaintiffs have more than sufficiently alleged "loss." In addition to alleging interruption of service, Plaintiffs also allege losses to GPP "including the cost of responding to Defendants' individual and/or collective offenses, conducting damage assessments, restoring the data, program, system and/or information to its condition prior to Defendants' offenses, lost revenue . . . . GPP has suffered losses in excess of $5,000 in aggregate value as a result of Defendants' course of conduct". Complaint, ¶¶ 36, 46. Plaintiffs also have alleged losses by Ms. Friess Yessin: "including the cost of responding to Defendants' individual and/or collective offenses, conducting damage assessments, guarding against future intrusions, incurring attorneys' fees in responding to and protecting against further intrusions, which attempts are ongoing. Ms. Friess

Yessin also has incurred losses in her bargaining position in the divorce proceedings against Defendant, as her settlement integrity has been compromised by Defendants' unlawful surveillance of her privileged communications with her counsel. Ms. Friess Yessin has suffered losses in excess of $5,000 in aggregate value as a result of Defendants' course of conduct". Complaint, ¶¶ 37, 47.

At the pleadings stage, Plaintiffs are not required to provide receipts or quantify all their "losses." As set forth above, Plaintiffs have sufficiently alleged "loss" under the statute.

2. Plaintiffs Have Alleged "Damages"

In accordance with Section 1030(g), Plaintiffs also have sufficiently alleged "damages". Section § 1030(e)(8) defines "damages" as "any impairment to the integrity or availability of data, a program, a system or information." Section § 1030(g) generally permits a plaintiff to recover "economic damages," which is not explicitly defined by statute, but which, the Fourth Circuit held in *iParadigms*, "ought to be accorded its ordinary meaning, which would include consequential damages but exclude recovery for pain and suffering or emotional distress." 562 F.3d at 646 (*citing Creative Computing v. Getloaded. com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) (concluding that the "economic damages" includes "loss of business and business goodwill")). Plaintiffs have alleged such economic damages, not only in the paragraphs discussed above (36, 37, 46 and 47), but also in paragraphs 38 and 48 (noting that both parties suffered economic damages, including "but not limited to lost profits, lost goodwill, damage to reputation, and impairment of value to property in amounts to be proven at trial." These allegations are more than sufficient and the precise damages will not be known until discovery is completed.

In addition, without citing any legal authority, Defendant asserts that "mere surveillance

of data will not support a damage claim." Motion at 14. Plaintiffs do not allege mere surveillance. Plaintiffs allege—as recited throughout this section --specific harm to the GPP system and Ms. Friess Yessin as a result of Defendant's unlawful conduct. Defendants cite no authority to support the contention that Defendant's ill-gotten advantage in the divorce proceedings, by compromising Ms. Friess Yessin's negotiating position in intercepting and surveilling her privileged communications with her counsel, does not constitute "damages" or "economic damages" under the statute.

Because Plaintiffs have sufficiently alleged "damage" and "loss", Defendant's Motion should be denied. Nevertheless, out of an abundance of caution, Plaintiffs have amended their claims to provide more detail related to the nature of their loss and damages. *See* Amended Complaint ¶¶ 36, 37, 46, 47, 54, 55, 62, 63, 70, 71.

IV. Plaintiffs Have Stated Claims Under The ECPA – Counts VI And VII

In his Motion, Defendant asserts that Plaintiff has not stated claims under the ECPA – Counts VI and VII – solely because he was "authorized" to access the GPP computer system. Motion at 14. As set forth above, because Defendant had no such authority, Defendant's Motion should be denied. *See* Sections II-III, s*upra*.

The ECPA makes it an offense to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided, or intentionally exceed[ ] an authorization to access that facility; and thereby obtain[ ], alter[ ], or prevent[ ] authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701. As with the CFAA counts (Section III, *supra*), Plaintiffs have stated claims against Defendant by alleging that he, without any authorization from Plaintiffs, accessed password-protected areas of GPP's computer system, including Ms. Friess Yessin's email account. Defendant has cited no

authority that supports the principle that a Manager who intentionally accesses a computer network after misappropriating the username and password of an authorized user cannot be liable under the ECPA. On the facts alleged here, the ECPA claim is adequately alleged against Defendant, who was never authorized by GPP to access its computer system or network, much less Ms. Friess Yessin's GPP email account. Complaint, ¶¶ 10, 12, 14, 16, 27, 31, 33, 35, 41, 43-45, 51, 59, 67, 75, 83, 92, 99, 106, 113, 121-22, 131-33.

Although Plaintiffs have been unable to find any cases which address the precise factual scenario presented here, *i.e.*, one Manager of a LLC misappropriating the username and password of another Manager in order to access the company's computer network and the other Manager's email account without her knowledge or authorization, courts have found liability under the ECPA and CFAA in analogous situations. For instance, courts have generally held that a violation of the ECPA occurs when an employee intentionally accesses his co-workers' email accounts without authorization. *Bloomington-Normal Seating Co., Inc. v. Albritton*, 2009 U.S. Dist. LEXIS 40302, * 10 (C.D. Ill. May 13, 2009) (holding that plaintiff had adequately stated claims under the CFAA and ECPA where it alleged that a former employee had accessed confidential company information, including his manager's email, without permission); *Cedar Hill Associates, Inc. v. Paget*, 2005 U.S. Dist. LEXIS 32533, *7 (N.D. Ill. Dec. 9, 2005) (denying defendant's motion for summary judgment where it seemed clear that he intentionally accessed his coworkers' e-mail accounts without authorization and therefore in violation of the ECPA); *Cardinal Health 414, Inc. v. Adams*, 582 F. Supp. 2d 967, 977 (M.D. Tenn. 2008) ("where the facts indisputably present a case of an individual logging onto another's email account without permission and reviewing the material therein, a summary judgment finding of an [ECPA] violation is appropriate.") (internal citation omitted).

These cases are analogous – if one employee does not have authorization to spy on another employee, a Manager of a LLC does not have authorization to spy on another Manager. Because Defendant was not authorized to conduct the unlawful surveillance alleged in Plaintiffs' Complaint, his Motion should be denied. *See* Section II-III, *supra*.

V. Plaintiffs' Have Stated Claims Under The VCAA – Counts XII And XIII

In his Motion, Defendant asserts that Plaintiff has not stated claims under the VCAA because: (1) Defendant was "authorized to access the GPP computer system and the information it contained;" and (2) "there is no allegation that Defendant "obtained, embezzled, or converted" Plaintiffs' property and "viewed her employment or other financial information." Motion at 14-15.

A. Defendant Did Not Have Authorization.

As discussed at length in Sections II-IV above, Plaintiff has specifically alleged that Defendant did not have authority to conduct the unlawful interception and surveillance alleged in the Complaint, and those allegations must be accepted as true. In addition, Plaintiffs explicitly allege, under Counts XII and XIII, that Defendant acted without authority. Complaint ¶¶ 121, 122, 123, 131, 132, 133.

B. Plaintiffs Have Sufficiently Alleged The Elements Of The Virginia Computer Crimes Act

1. Va. Code § 18.2-152.3

To state a claim under section 18.2-152.3,[6] Plaintiffs must allege that Defendant: (1) used a computer or computer network; (2) without authority; (3) intending to obtain, embezzle, or convert the property of another. Va. Code § 18.2-152.3; *Othentec Ltd. v. Phelan*, 526 F.3d

[6] Virginia Code § 18.2-152.12 grants civil recourse to a party aggrieved under, *inter alia*, §§ 18.2-152.3 and -.5

135, 140 (4th Cir. 2008). To dismiss this claim, Defendant argues that "there is no allegation that Mr. Yessin 'obtained, embezzled, or converted' Mrs. Yessin's property or GPP property to his own." Motion at 15. This is simply untrue. In the Complaint, Plaintiffs specifically allege that Defendant "intercepted and surveilled Ms. Friess Yessin's communications with GPP executives, personnel, clients and business partners, as well as her privileged communications with her counsel," and that "[t]hese actions constitute conversion of the property of Ms. Friess Yessin and GPP, and the obtaining of property by false pretenses." Complaint, ¶¶ 121-22. Defendant has not cited any authority to support the contention that such actions do not constitute conversion or obtaining property by false pretenses. Indeed, *Barnes v. Commonwealth*, 2000 Va. App. LEXIS 204 at *6 (Va. App. 2000) provides that these elements must be liberally construed. In *Barnes*, the court upheld the conviction of a former police officer who was charged under this statute for using the state computer system to check the VIN number of a car that her brother had stolen. *Id*. Although Barnes argued that, as a police officer, she was authorized to use the system, the court upheld the trial court's finding that Barnes acted "without authority" and under "false pretenses" to assist her brother in retaining a stolen car. *Id*. If the police officer's actions in *Barnes* satisfies the "without authority" and "false pretenses" elements of Va. Code § 18.2-152.3 (where a police officer has access to the system for proper purposes, but not illegal ones), then certainly Defendant's conduct—where he was wholly unauthorized to be on the GPP system—satisfies this standard as well. Hence, Plaintiffs have stated a claim for computer fraud under Va. Code § 18.2-152.3.

2. **Va. Code § 18.2-152.5**

To state a claim under Va. Code § 18.2-152.5, Plaintiffs must allege: (1) the use of a computer or computer network by the offender; (2) with the intent to examine another's records;

(3) in an unauthorized context when the offender knew or should have known that he was without authority to examine the records; and (4) the records so examined contain employment, financial, or personal information of the pleader. *S.R. v. INOVA Healthcare Services*, 49 Va. Cir. 119 (Fairfax Co. 1999); *Plasters v. Commonwealth*, 2000 Va. App. LEXIS 473, at *3 (Va. App. June 27, 2000) (unpublished opinion); *Albertson v. Albertson*, 73 Va. Cir. 94, 96 (Fairfax Co. 2007). "Examination" under this section "requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed." Va. Code § 18.2-152.5(A). Once again, Defendant cites no authority to support the argument that Plaintiffs have not stated a claim under this section.

In *INOVA Healthcare Services*, a patient (a nurse at Fairfax Hospital who chose to be admitted to Alexandria Hospital to maintain her privacy) sued INOVA and two other nurses at Fairfax Hospital under this statute for improperly accessing her medical records. The defendants demurred, claiming that plaintiff failed to allege that the defendants lacked authority to examine her personal medical information. 49 Va. Cir. at 129. Specifically, the defendants contended that assuming, *arguendo*, they did access her medical records through the computer system, plaintiff's claim rested on the incorrect assumption that a hospital is without authority to view the records of its own patients. *Id*.

The court disagreed. *Id*. at 130. The court focused on the fact that defendants examined plaintiff's records "at a time when review of these records was not reasonably related to the rendering of health care services." *Id*. It held that a plain-meaning analysis of the statute demonstrates that it is not aimed at preventing businesses from accessing confidential information necessary to effectively conduct business, rather, it is aimed at preventing the

unauthorized examination of personal information. *Id*. Accordingly, the court overruled defendants' demurrer to plaintiff's claim for Computer Invasion of Privacy. *Id*. at 131.

Similarly, Defendant's improper conduct under this statute has been properly alleged. Plaintiffs allege that Defendant "used the computer, email system and computer network provided by GPP to Ms. Friess Yessin, for use at her home, to examine financial, personal and privileged information relating to GPP, its officers and employees, and/or Ms. Friess Yessin," and that they "used the computer, email system and computer network provided by GPP to Ms. Friess Yessin in an unauthorized context, where they knew or should have known that they lacked authority to do [so]." Complaint, ¶¶ 132-34. More specifically, Plaintiffs have alleged that "[w]ithout authorization or consent, Defendant broke into Ms. Friess Yessin's GPP email account and unlawfully surveilled her business and personal documents and communications, including very sensitive, privileged communications with her counsel regarding her strategy in her impending divorce proceedings with Defendant." *Id*. at ¶ 16; *see also id.* at ¶¶ 33, 35, 43-45, 51, 59, 67, 75, 83, 92, 99, 106, 113, 121-22. Accordingly, Plaintiffs have stated claims under the Virginia Computer Crimes Act, and Defendant's Motion should be denied.

VI. Plaintiffs Have Stated Claims Under The FWA – Counts III, IV And V

In his Motion, Defendant asserts that Plaintiff has not stated claims under the FWA – Counts III, IV and V – solely because Plaintiff has not alleged that Defendant "intercepted" any electronic communications during transmission" (and only alleged that Defendant accessed "previously transmitted communications stored in GPP's computer"). Motion at 17-19. The entire premise of this argument is in error - in accordance with Rule 8(d), Plaintiffs have alternatively alleged that Defendant intercepted electronic communications that were acquired during transmission ***and*** that were previously transmitted communications that were stored.

Because Plaintiffs have sufficiently alleged both, Defendant's Motion should be denied.

Defendant relies on *Fraser v. Nationwide Mut. Ins. Co*., 135 F. Supp. 2d 623, 633-34 (E.D. Pa. 2001), for the proposition that an interception under the Wiretap Act occurs "during the transfer, or during the course of transmission." An interception, the Court held, "occurs when transmission is interrupted, or in other words when the message is acquired after it has been sent by the sender, but before it is received by the recipient. The point in time when the message is acquired is the determining factor for whether or not interception has occurred." *Id*. at 634. Analogizing to the interception of a voice mail message left on a recipient's voice mail system, the Court stated, "if a third party obtains access to the recipient's mailbox and retrieves a message before it has been heard by the recipient, there is interception." *Id*. (*citing United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998)). "Retrieval of an e-mail message from either intermediate or back-up storage is interception; retrieval of an e-mail message from post-transmission storage, where the message remains after transmission is complete, is not interception."[7] *Id*. In *Fraser*, it was undisputed that the Defendant acquired the email by retrieving it from the system—from post-transmission storage—after the plaintiff had read it: "Fraser does not allege that Nationwide retrieved his e-mail communication before it was received and read by the recipient. Nationwide acquired Fraser's e-mail from post-transmission storage, after transmission was complete. Therefore, there was no 'interception.'" *Id*. at 635.

[7] When a party sends an email, the system from which it is sent stores a copy of the message for back-up protection, and also in temporary storage. *Fraser*, 135 F. Supp. 2d at 633-34. The *Fraser* Court referred to these events as "intermediate storage" and "back-up protection storage." *Id*. The email then passes through various waypoints en route to its destination, and a copy of it is again stored at each of these points, in back-up and intermediate storage. *Id*. Once the message arrives at its destination, and "is retrieved by the intended recipient," the message is copied into another type of storage, which the *Fraser* Court referred to as "post-transmission storage." *Id*. Transmission of an email may take as little as seconds or minutes. An email may remain in post-transmission storage for years. *Id*.

Plaintiffs' allegations stand in contrast to *Fraser*, and in total contradiction to Defendant's characterization of them. By again ignoring the allegations of Plaintiffs' Complaint and failing to cite to them, Defendant strains to portray the Complaint in a manner that fits within his argument. He summarily concludes, without pointing to any actual language or paragraph of the Complaint, that "Plaintiffs merely allege that Mr. Yessin accessed previously transmitted communications stored in GPP's computer" (Motion at 18) and "Plaintiffs merely allege that Mr. Yessin . . .retrieved e-mails that had already been delivered to and stored in GPP computer system." *Id*. at 19. To the contrary, the Complaint specifically alleges that some of the e-mails acquired by Defendant were in transit, as it states that "[i]n the course of Defendant's illicit surveillance, he read other correspondence between Ms. Friess Yessin and her counsel; ***some of which had not yet been read by the intended recipient***, and some of which already had been read by the intended recipient." Complaint ¶ 17 (emphasis added.) As the *Fraser* Court stated, an interception occurs after an email has been sent, but "before it has been received by the recipient." 135 F. Supp. 2d at 634. The Complaint further alleges that Defendant "intercepted" Plaintiffs' electronic communications, in violation of the Wiretap Act, numerous other times throughout the Complaint. Complaint, ¶¶ 3-4, 24-25, 51, 59, 67, 92, 99, 106, 113, 121, 122, 145. In so doing, Plaintiffs have satisfied the pleading requirement of Fed. R. Civ. P. 8 by providing "a short and plain statement of the claim showing that the pleader is entitled to relief." *Id*.[8]

[8] Defendant also cites *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994), for the proposition that an e-mail must be acquired during transfer in order to be intercepted. The Court in *Steve Jackson Games* –after a full trial—found that the emails at issue, although unread by the Defendant, were on the computer hard drive of the electronic bulletin board to which messages were posted, and were in "electronic storage"-- not "in transit"-- despite being unread by the recipient. Because the definition of electronic communications, unlike the definition of wire communications, does not include "electronic storage of such communications," the Court held that emails acquired while in such storage cannot be "intercepted." Whether the emails at issue in this case were in electronic storage or

Nevertheless, out of an abundance of caution, Plaintiffs have amended their Complaint to clarify that Defendant intercepted the electronic communications during the course of their transmission. Amended Complaint, ¶¶ 17, 24, 25, 51, 59, 67. *See also id.* ¶¶ 92, 99, 106, 113, 121, 122. Thus, even if Defendant's argument had any merit, it is now moot.

VII. Plaintiffs Have Stated Claims Under The VWS – Counts VIII, IX, X, And XI

In his Motion, Defendant asserts that Plaintiffs have not stated claims under the VWS - Counts VIII, IX, X, and XI -- solely because Plaintiffs have failed to allege the contents of a wire or electronic transfer during the course of its transmission," but instead "have only alleged that [Defendant] used [Ms. Friess Yessin's] login and password to gain access to emails that had been previously delivered." Motion at 19-20. As set forth in Section VI, because Plaintiffs have

---

not is a question of fact. In *Steve Jackson Games*, the case was decided after a full trial, *id*. at 457; it was not decided at the pleadings stage where all facts are construed in favor of Plaintiffs. *City of Goldsboro*, 178 F. 3d at 243-44. As explained above, Plaintiffs have sufficiently alleged that the emails are in transit because some of them had not yet been read or received by the intended recipient (Complaint, ¶ 17), and the Amended Complaint further clarifies this fact. (Amended Complaint, ¶¶ 17, 24, 25, 51, 59, 67). Second, Plaintiffs submit that this opinion, which is in any event not binding on this Court, was wrongly decided, and that the correct analysis on what constitutes an "interception" is set forth in the more recent decision of *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005). In *Councilman*, the court held that even electronic communications that are in certain types of electronic storage may still be "intercepted" within the meaning of 18 U.S.C. § 2511. The court held that the proper construction of the ECPA compelled the conclusion that even messages in "transient" electronic storage are still "electronic communications" that can be "intercepted" under the Act. 418 F.3d 79 ("An e-mail message does not cease to be an 'electronic communication' during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage."). Defendant also relies on *United States v. Simons*, 29 F. Supp. 2d 324, 329-30 (E.D. Va. 1998), which dismissed a claim under the Wiretap Act "because nothing in the record indicated that the e-mail was obtained while it was being transferred." However, in *Simons*, the opinion implies that the Defendant had long ago received and read the emails that were eventually seized. *Simons*, 29 F. Supp. 2d at 329. The remaining cases cited by Plaintiff deal with transmissions by pager or recorded phone conversation, and are relevant only for the proposition that an email must be "in transmission" to be intercepted. *See United States v. Turk*, 526 F.2d 654 (5th Cir. 1976) (decided prior to the codification of the ECPA, which updated the Wiretap Act); *United States v. Reyes*, 922 F. Supp. 818, 836 (S.D.N.Y.1996); *United States v. Meriweather*, 917 F.2d 955, 960 (6th Cir. 1990).

alternatively alleged that Defendant intercepted electronic communications that were during transmission and that were stored, and because Plaintiffs have amended their Complaint to provide more detailed facts as to how the interception occurred. Amended Complaint ¶¶ 92, 99, 106, 113, 121 and 122. Defendant's Motion should be denied.

VIII. <u>As Alleged In The Complaint, Plaintiffs Have Standing To Bring This Action</u>

Again relying upon interjected facts and false documents that are entirely outside the pleadings, Defendant asserts that Plaintiffs lack standing to bring this action because "[n]o meeting of the managers is alleged to have taken place, and of course, none ever took place." Motion at 22; *see also id.* at 21, 23. In essence, Defendant is again attempting to interject facts that are beyond the pleading (that a meeting was required) so he can then attempt to dispute them (a meeting was not held), which at best would raise a fact issue for discovery.

First, in their Complaint, Plaintiffs have alleged that "Ms. Friess Yessin is the Chief Executive Officer, a Manager, and a Principal of GPP. Mr. Weiss is the Chief Operating Officer, a Manager, and a Principal of GPP. Together, Ms. Friess Yessin and Mr. Weiss are the only officers and Principals of GPP. Ms. Friess Yessin and Mr. Weiss also are the majority owners and as 2 of the 3 Managers have majority control over GPP. As such, only Ms. Friess Yessin and Mr. Weiss have the authority to make decisions on behalf of GPP," which would include authorizing the filing and prosecution of this action. Complaint, ¶ 12. These facts must be accepted as true and Defendant cannot dispute them in a Rule 12(b)(6) motion. Moreover, Defendant cites no authority for the proposition that Plaintiffs were required to allege in their Complaint that a meeting was held and that a majority of the Managers and/or Members authorized this action, and Plaintiffs are not aware of any such authority.

Second, under the governing law, no such meeting would be required. When this action

was filed, Ms. Friess Yessin and Mr. Weiss were the majority Members and 2 of the 3 Managers. Florida law provides that "[a]ction requiring the consent of members or managers under this chapter may be taken without a meeting, subject to the limitations of section 608.4231." Fla. Stat. Ann. § 608.422(5). Section 608.4231(8) provides that "the members may take such action without a meeting, without prior notice, and without a vote if a consent or consents in writing, setting forth the action so taken, are signed by the members having not less than the minimum number of votes that would be necessary to authorize or take such action at a meeting, but in no event by a vote of less than a majority-in-interest of the members that would be necessary to authorize or take such action at a meeting." Fla. Stat. Ann. § 608.4231(8). Thus, as the majority Members, Ms. Friess Yessin and Mr. Weiss could and did consent in writing, authorized the filing of this lawsuit without a meeting, and provided Defendant notice.

Third, on August 18, 2009, as the majority Members, Ms. Friess Yessin and Mr. Weiss consented in writing to remove Defendant as a Manager as a result of, *inter alia*, the fraudulent Annual Reports he filed, the computer crimes alleged in Plaintiffs' Complaint, and Defendant's breaches of fiduciary duty, and provided notice of this consent to Defendant *See* Fla. Stat. Ann. § 608.4231(8); *see also* Fla. Stat. Ann. § 608.422(4)(c)(1) (a Manager "[m]ust be . . . removed, or replaced by a vote, approval or consent of a majority-in-interest of the members . . ."). Thus, as the only Managers and a Majority of the Members, only Ms. Friess Yessin and Mr. Weiss could and did authorize the filing of the Original and Amended Complaints.

Although Plaintiffs contend that they have more than met the requirements of Rule 8, out of an abundance of caution, in their Amended Complaint Plaintiffs augment their allegations to address Defendant's concerns and add, among other things, that as the only Managers and majority Members, Ms. Friess Yessin and Mr. Weiss conducted a meeting, approved by consent

the continuation of this action and the filing of the Amended Complaint, and provided Defendant notice (in accordance with Fla. Stat. Ann. § 608.4231). Amended Complaint, ¶ 12. Thus, to the extent there was any merit to Defendant's standing argument, it is now moot.

IX. This Action Should Not Be Stayed

Finally, in his Motion, Defendant contends that this action should be stayed pending resolution of the frivolous declaratory relief action that he filed ***after*** Plaintiffs filed and served this action. Motion at 23-25 & Exhibit 3. To make this argument, Defendant again interjects facts that are beyond the pleadings (including the false Annual Reports he submitted) and, based upon these improperly interjected facts, contends that there is a "bona fide dispute regarding who may manage GPP, *i.e.*, whether [Plaintiff] Friess and Jeffrey Weiss are the Managers of GPP or whether [Defendant] Yessin is the sole manager of GPP . . . ." Motion at Exhibit 3, ¶ 18; *see also id*. at Wherefore Clause, ¶¶ 1-2.[9]

As discussed in Sections II(B) & VIII above, there is no dispute (much less a bone fide one) as to who GPP's Managers and Members are and whether they could authorize this action. Put simply, Defendant cannot file a baseless State court action (that is premised on the knowingly false Annual Reports) ***after*** this action was properly filed and served in order to stay

[9] For instance, Defendant interjects that "he caused GPP to be incorporated", "[h]e then provided working capital for the Company", "he also loaned the Company $100,000 and $50,000 to fund its operations", "[h]e also advanced the Company additional funds to pay GPP's expenses", and "an operating agreement was prepared and agreed to by all members, which was signed by Mr. Yessin and which listed him as the sole manager of the Company." Motion at 24. All these facts are beyond the pleadings and, as discovery would reveal, almost entirely untrue. For instance, while he gave GPP some funds, he did not cause GPP to be incorporated. Moreover, the Operating Agreement that Defendant refers to and which is the basis of his declaratory relief action was not agreed to or signed by Ms. Friess Yessin or Mr. Weiss; in fact, they had never even seen it or discussed its contents before the declaratory relief action was served upon them. As set forth above, as at best a minority Member and only 1 of 3 Managers, Defendant cannot alone dictate the terms of, and execute, the Operating Agreement – it is an agreement that must be agreed to by all the Members and/or Managers. *See* Section II(B), *supra*.

these proceedings and wrest this Court of its federal question jurisdiction.

Moreover, a party seeking a stay must justify it by "clear and convincing circumstances," and must make out a "clear case of hardship or inequity in being required to go forward. . . . Otherwise, a stay is not merited." *JTH Tax, Inc. v. Whitaker*, 2007 U.S. Dist. LEXIS 52672 at *16 (E.D. Va. July 16, 2007). As explained above, Defendant has made no such showing here. Finally, in accordance with the first-filed doctrine, this Court should retain jurisdiction to resolve Plaintiffs' claims. *Affinity Memory & Micro, Inc. v. K&Q Enterprises, Inc.*, 20 F. Supp. 2d 948, 954 n.10 (E.D. Va. 1998). Principles of comity and judicial economy dictate that the Court follow the first-to-file rule. *Ulmet v.United States*, 888 F.2d 1028, 1031 (4th Cir. 1989). Put simply, Defendants' request for a stay is forum-shopping at its worst, and should not be tolerated.

CONCLUSION

For the forgoing reasons, Defendant's Motion should be denied in its entirety.

Dated: September 17, 2009

Respectfully Submitted,

PLAINTIFFS
By Counsel

/s/

Bernard J. DiMuro, Esq.
Virginia State Bar # 18784
Stephen L. Neal, Jr., Esq. (*pro hac vice*)
Stacey Rose Harris, Esq.
Virginia State Bar #65887
Counsel for Plaintiff
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: (703) 684-4333
Fax: (703) 548-3181
E-Mails: bdimuro@dimuro.com;
sneal@dimuro.com; sharris@dimuro.com

CERTIFICATE OF SERVICE

I hereby certify that on this 17th day of September, 2009, I electronically filed the foregoing Plaintiffs' Opposition To Defendant's Motion To Dismiss with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following counsel of record:

Charles M. Sims, Esq.
Counsel for Defendants
LeClairRyan
951 East Byrd Street, 8th Floor
Richmond, VA 23219
Phone: (804) 343-5091
Fax: (804) 783-7655
Email: charles.sims@leclairryan.com;

C. Matthew Haynes, Esq.
Counsel for Defendants
LeClairRyan
225 Reinekers Lane, Suite 700
Alexandria, VA 22314
Phone: (703) 647-5919
Fax: (703) 647-5989
Email: matthew.haynes@leclair.com

/s/
Bernard J. DiMuro, Esq.
Virginia State Bar # 18784
Stephen L. Neal, Jr., Esq.
(*pro hac vice*)
Stacey Rose Harris, Esq.
Virginia State Bar #65887
Counsel for Plaintiffs
DiMuroGinsberg, P.C.
908 King Street, Suite 200
Alexandria, VA 22314
Phone: (703) 684-4333
Fax: (703) 548-3181
E-Mails: bdimuro@dimuro.com;
sneal@dimuro.com; sharris@dimuro.com